

CHAPTER IX. PRIVACY AND FAIR INFORMATION PRACTICES

As indicated in Chapters I and II, a major concern about the Basic Pilot program is that it would provide increased opportunities for invasion of privacy and breaches of confidentiality. This chapter discusses “fair information practices,” a broad term that encompasses issues of privacy, confidentiality, and computer security. The discussion focuses on the extent to which employer and Federal Government safeguards are sufficient to ensure the security and privacy of confidential information about employees. It also makes recommendations for changes to the Basic Pilot program that would improve system security.

A. EMPLOYER SAFEGUARDS

As a condition of participating in the Basic Pilot, all employers sign a Memorandum of Understanding (MOU) that includes the following provisions in the section on employer responsibilities:

“The Employer agrees that it will use the information it receives from the SSA or the INS pursuant to the Basic Pilot and this MOU only to confirm the employment eligibility of newly-hired employees after completion of the Form I-9. The Employer agrees that it will safeguard this information, and means of access to it (such as passwords) to ensure that it is not used for any other purpose and as necessary to protect its confidentiality, including ensuring that it is not disseminated to any person other than employees of the Employer who need it to perform the Employer’s responsibilities under this MOU.

“The Employer acknowledges that the information which it receives from SSA is governed by the Privacy Act (5 U.S.C. §552a(i)(1) and (3)) and the Social Security Act (42 U.S.C. 1306(a)), and that any person who obtains this information under false pretenses or uses it for any purpose other than as provided for in this MOU may be subject to criminal penalties.”

1. SECURE USE OF THE BASIC PILOT SYSTEM

As stated in the MOU, safeguards must exist within each establishment to ensure that unauthorized persons cannot access the system. The Basic Pilot manual specifies that each person conducting queries should have his/her own user ID and password and that passwords belonging to persons no longer using the system be reported to the INS Help Desk for deactivation. For further security, users must change their passwords every 45 days to maintain access to the system. Additionally, employers are required to install the Basic Pilot software on non-networked computers, so that the only possible operator must be physically present at the computer on which the software is installed.

Members of the evaluation team who interviewed employers in their establishments observed considerable differences in the ways employers implemented these safeguards. Some employers appear to place stringent limits on system access by keeping the computer, software, and instructions in a locked office accessible only by authorized persons. However, observers also noted cases in which it would be very easy for an unauthorized person to obtain an employee's work-authorization status by accessing the computer containing the pilot system on the employer's premises.

Based on observations during on-site visits to a sample of participating establishments, computers were located in rooms that could be locked in approximately 60 percent of the cases. Of these, 38 percent were not actually locked at the time of the site visit, which took place during normal business hours. Only 22 percent of employers stored the pilot system instructions in a locked drawer or other secure location, and approximately half kept them in plain sight (Exhibit IX-1).

Exhibit IX-1: Where Employers Keep Basic Pilot Instructions

Where Instructions Are Stored	Percent of Employers
Locked secure location	22
Out of sight	22
Not next to computer	32
Next to computer	15
Other	9

SOURCE: On-Site Employer Survey

Employers were generally more cautious about password security. In 68 percent of the establishments, the person responsible for using the system had memorized the password, 7 percent of employers stored the password in a locked drawer or another secure location, and 15 percent kept the password out of sight. However, 10 percent kept the password in clear view (Exhibit IX-2).

Exhibit IX-2: How Employers Handle Basic Pilot System Passwords

How Password Is Handled	Percent of Employers
Clerk memorized password	68
Out of sight	15
Locked secure location	7
Next to computer	5
In sight but not next to computer	5

SOURCE: On-Site Employer Survey

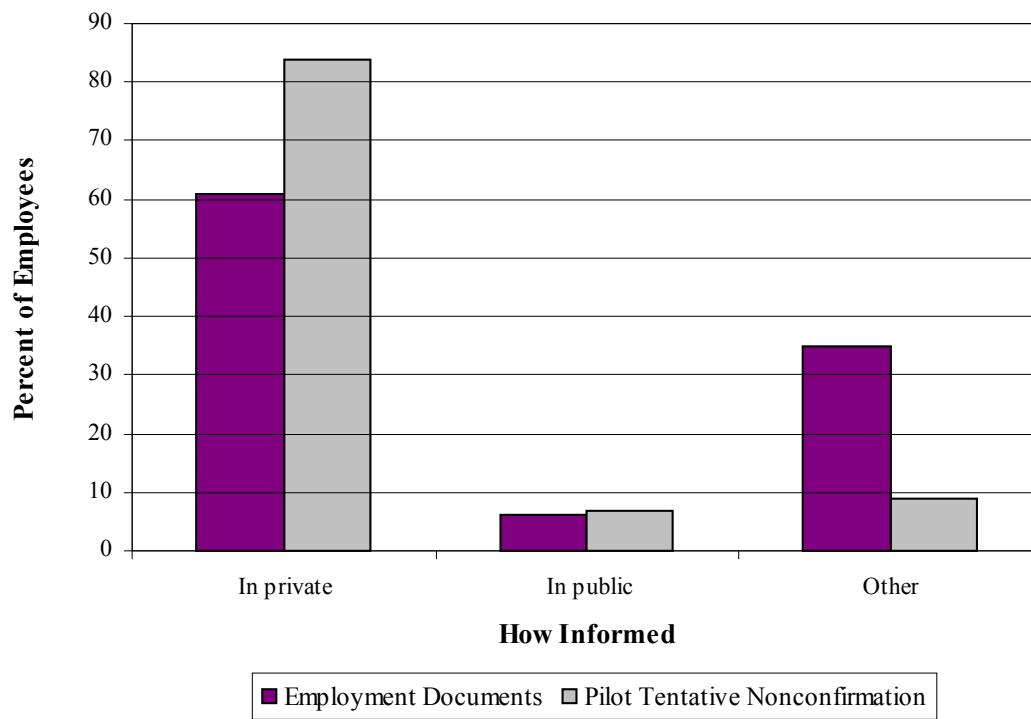
The reasons for breaches in employer security in protecting the dedicated computer, pilot instructions, and passwords were not specifically addressed during the on-site visit. Breaches in security may be attributable to insufficient emphasis on system security in the Basic Pilot system training materials, a lack of concern regarding privacy issues on the part of employers, or the impracticality of the required level of security in the environment of a human resources department.

2. PRIVACY OF EMPLOYEE INFORMATION

In addition to potential misuse of the pilot computer system itself, authorized or unauthorized users could violate employees' privacy in the way that they administer the pilot system. For example, employers may tell employees about tentative nonconfirmations in a setting that is not private, perhaps letting other employees know. To determine whether such violations are occurring, the evaluation team asked employees how they were told about problems with their work authorization.

Among pilot employees who were told about problems with their employment documents (n=101), 61 percent reported that they were informed in private with no one else around. Among employees who were told about a tentative nonconfirmation of employment authorization, 84 percent reported that they were informed in private with no one else around. Although the majority of employers appear to have informed their employees of confirmation difficulties in private, some employers did not protect their employees' rights to privacy (Exhibit IX-3).

Exhibit IX-3: How Employees Were Informed of Employment Verification Problems



SOURCE: Employee Interviews

B. FEDERAL SAFEGUARDS

Federal officials interviewed about the security of the pilot computer system reported that privacy was uppermost in the minds of those who created the pilot programs. In designing the Basic Pilot system, SSA and INS created multiple barriers to unauthorized access to their systems and used technical safeguards. These safeguards included assigning user IDs and passwords to specific individuals and permitting access to the pilot system only on dedicated computers and communication lines. By these means, the authentication of user information could be tied to a specific communication line and personal computer (PC). INS officials also pointed out that the verification system was designed to contain and require a minimum amount of information and to return limited information on work-authorization status. According to these Federal officials, the following procedures are currently used to ensure the security of Federal system files accessed by the Basic Pilot:

- *recognizing and performing queries only for authorized employers who have signed an MOU and taking security precautions to restrict employer access to the Basic Pilot database.* This security is accomplished through the use of establishment-level access codes and individual user IDs and passwords. These passwords must be renewed every 45 days for continued use of the Basic Pilot system.
- *limiting the information on the Federal database accessed by employers to the minimum necessary to operate the pilot program and confirm work authorization.* Employers do not have access to the full SSA or INS databases. The Basic Pilot data are transmitted over a secure line to SSA or INS; at this point, the system emulates the process of accessing the SSA or INS database by presenting the user with a screen requiring a user ID and a password. Other than information on work-authorization status, the system ultimately provides no information that the employer does not already have.
- *taking precautions against misuse of the SSA Numerical Identification File (NUMIDENT) and INS Alien Status Verification Index (ASVI) databases by Federal employees and contractors.* Since the security safeguards used for these databases in the Basic Pilot are the same as those for other SSA and INS databases containing much more detailed information, it is doubtful that Federal employees misuse confidential information from the databases accessed by the Basic Pilot system. Additionally, the link between INS and the contractor administering the ASVI system is unidirectional, so the contractor does not have access to other INS databases.
- *electronically capturing Basic Pilot transactions.* The Basic Pilot transaction database captures employer query data that can be used to monitor employer actions and detect irregularities in system use, including potential misuse or abuse of the system. Although INS does some monitoring of employers through the transaction database, INS has not systematically used the captured data to detect system misuse.

C. SECURITY CHECKS

To determine how effective the current Federal measures are in protecting the program databases, the evaluation team tested Basic Pilot system security. Research assistants with an intermediate knowledge of computer operations played the role of system users.

The team performed tests in two areas:

- *Security*: whether unauthorized users can operate the Basic Pilot system by circumventing the user ID and password combination
- *Fraud*: whether it is possible to manipulate the computer system to provide false proof or documentation of work authorization

In both tests, the basis for determining how the system operates – and thereby for discovering ways to circumvent the system requirements – involved looking for system operating files using Windows Explorer, a standard software program available on most computers.

1. ACCESS TO USER ID AND PASSWORD

The system security test confirmed that a user ID and password are indeed necessary for employers to access the Federal databases used for employment verification in the Basic Pilot program. However, a weakness in system security was identified: A file in the system folder of the employer's PC contains a record of the user's access code, the user ID, and the password, which can be accessed to circumvent these protections. The file provides a troubleshooting log of each completed transaction that is overwritten by a new file whenever the Basic Pilot program is used. The evaluation team was able to view this file using a standard editing/word processing program. The file contained encoded information documenting the modem transmittal, as well as a line containing the access code, user ID, and password. The information appeared as follows:

```
$27288099$ 04WAITFORB  
_1_33_10_PVMD1016@ANUH@6343@@38400_02__
```

where "PVMD1016" is the access code, "ANUH" is the user ID, and "6343" is the password. The team's computer systems staff believed that this information would be accessible and understandable to someone with an intermediate knowledge of computer operations.

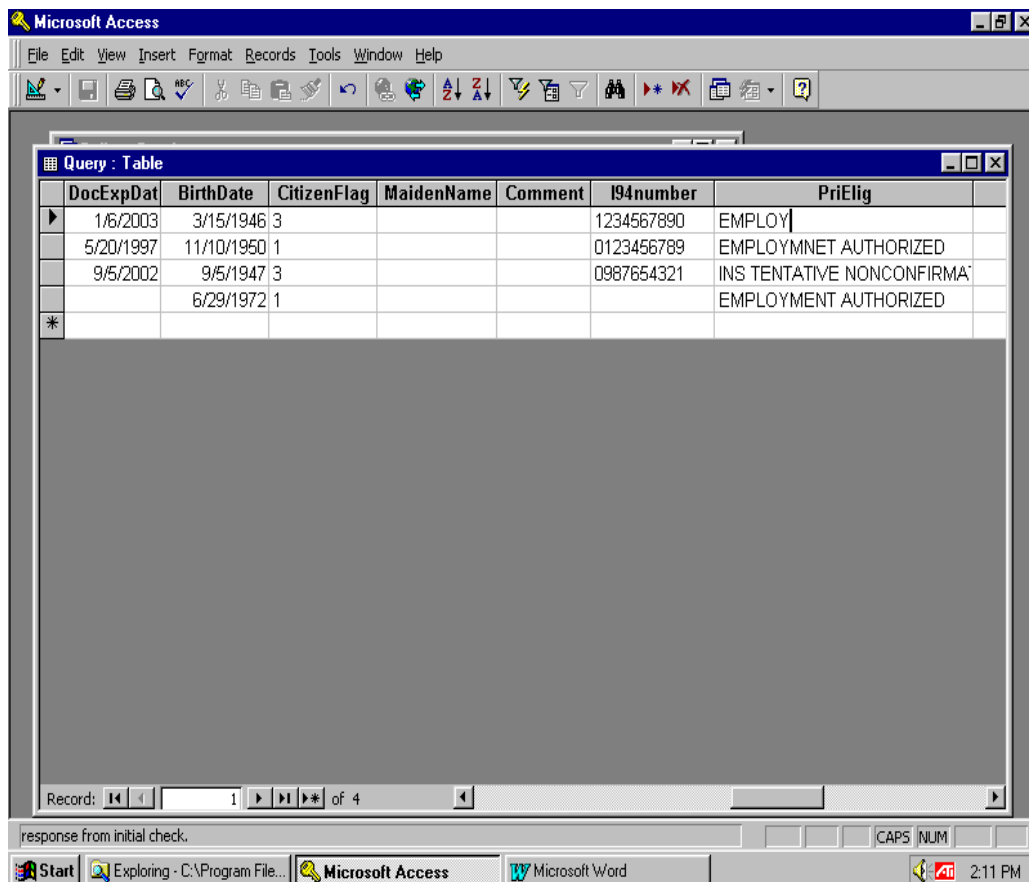
Thus, someone with access to an employer's PC could, at least in theory, obtain the user ID and password from the system file and use it to access the Federal databases used by employers for Basic Pilot employment verification.

2. MANIPULATING WORK-AUTHORIZATION DATA FOR PRINTABLE DOCUMENTATION

The evaluation team also tested whether someone could use the computer with the Basic Pilot software to falsify the system-generated Case Detail printouts that document the work-authorization result.¹²³ The testing staff easily located the Microsoft Access database file that stores the unencrypted data from automated queries, by browsing the directory and file structure using Windows Explorer. This Microsoft Access database was easily opened, and there were no restrictions on altering and then saving the results of the queries in this spreadsheet-type database.

Two methods of changing an employee's authorization status were found. The first method is to change the eligibility status of an employee by altering the "I94number" and "PriElig" (Primary Eligibility) fields in the Microsoft Access database table, as seen in Exhibit IX-4.

Exhibit IX-4: Manipulating the Primary Eligibility (PriElig) Field



DocExpDat	BirthDate	CitizenFlag	MaidenName	Comment	I94number	PriElig
1/6/2003	3/15/1946	3			1234567890	EMPLOY
5/20/1997	11/10/1950	1			0123456789	EMPLOYMNET AUTHORIZED
9/5/2002	9/5/1947	3			0987654321	INS TENTATIVE NONCONFIRMA
	6/29/1972	1				EMPLOYMENT AUTHORIZED

¹²³ Employers participating in the Basic Pilot are required to retain a paper copy of the Basic Pilot result, in addition to the Form I-9, as proof of "best efforts" to confirm work authorization, in case of any allegation of unlawful employment during an INS audit.

Data from this database can be modified and then displayed in the Case Detail (Exhibit IX-5) so that an employee originally confirmed as “Employment Unauthorized” appears as “Employment Authorized.” In other words, the system does not appear to have encoded restrictions on data modification. The Basic Pilot system simply displays the modified data, which the user can print and retain in the employee’s paper file. The user may close out this type of case as an “Invalid Query” or employee “Self-Terminated.” The user may also delete the row of data corresponding to the query for that employee within the Microsoft Access file, thus deleting all on-site records that the employee was processed through the system.

Exhibit IX-5: Appearance of Case Detail from Within the Basic Pilot Integrated System

The screenshot shows the 'Basic Pilot - [Case Detail]' window. The title bar includes 'File', 'Windows', 'System', and 'Help'. The menu bar contains 'Primary Query', 'Display Cases', 'Check for Responses/Send Queries', and 'Exit'. The main form area contains the following fields and controls:

- Last Name:** JONES
- First Name:** JOHN
- M.I.:** D
- Verification Number:** 200018014501801
- Maiden Name:** (empty field)
- Social Security #:** 000-00-0000
- Employee Status:**
 - ☒ A citizen or national of the United States
 - ☐ A Lawful Permanent Resident ...
 - ☐ An alien authorized to work ...
- Document type:** Unexpired Foreign Passport
- Document Expiration Date:** 05/20/1997
- Date of Birth:** 11/10/1950
- Hire Date:** 11/01/1997
- INITIAL ELIGIBILITY:** EMPLOYMENT AUTHORIZED
- SECOND ELIGIBILITY:** (empty field)
- Buttons:**
 - SSA Resubmit
 - SSA Referral
 - JNS Referral
 - Resolve Case
 - Request Addl Verification
 - Print This Case
 - Return to Display Cases

The taskbar at the bottom shows the Start button, Microsoft Word, and the Basic Pilot - [Case Detail] window. The system clock shows 2:13 PM.

The second method of changing the authorization status of an employee is to modify the personal information in the query database. For instance, the user may replace the personal information of an authorized worker with the personal information of an unauthorized worker and print and retain the Case Detail that displays the employee as “Employment Authorized.”

In summary, the Basic Pilot database can be modified to falsify the printable documentation of the Basic Pilot authorization result. However, if the user creates a false record of eligibility or a false indicator of ineligibility in the employer’s system, the altered information would be inconsistent with the individual’s status on the pilot transaction database. Such illegal actions might be detectable through a review of the

centralized transaction database and an audit of employers' employee records. However, there are no quality control checks, and currently no monitoring of how employers use the system, making it unlikely that these inconsistencies would be detected at the present time.

To ensure privacy and minimize system abuse, it is highly recommended that data files on the employer's PC be encrypted, so that unauthorized users cannot easily obtain the system password and cannot edit the system output on the employer's PC.¹²⁴

3. CONFIRMING WORK AUTHORIZATION FOR PERSONS NOT COVERED BY THE BASIC PILOT

As stated in the MOU and the Basic Pilot procedures, employers may only verify newly hired workers. They may not verify the work-authorization status of previously hired employees, job applicants, or nonemployees. An area for potential abuse lies in the use of the verification system to obtain work-authorization information for persons not covered by the program. Although the MOU specifically prohibits prescreening of applicants, it is possible to enter information on any person into the system. As discussed in Chapter VII, there is evidence that some employers use the system to prescreen applicants. Since the system data are not always accurate or complete, and since job applicants would presumably not be given an opportunity to resolve their records, this is a violation of fair information practices.

The Basic Pilot system might also be used for illegitimate purposes such as determining whether a neighbor or customer is authorized to work. The unsecured physical status of the computers and passwords in some establishments increases the possibility that unauthorized users could use the system for such purposes. However, to complete a record check, a trespasser would need information on the person being verified, including his/her Social Security number and Alien Number. Without systematic audits of employer records in combination with the information captured in the Basic Pilot transaction database, it would not be possible to monitor these and other improper uses of the Basic Pilot system.

D. SUMMARY

The evaluation team examined issues of privacy and computer security related to the Basic Pilot and arrived at the following conclusions:

- There is little risk of pilot system misuse by Federal employees beyond the potential that exists because of their access to other INS and SSA databases. Any Federal employee or contractor wishing to obtain INS or SSA information for unauthorized purposes could obtain the same information from other Federal databases (e.g., the INS Central Index System) that contain more extensive personal information. Therefore, use of the pilot system increases risk only to the

¹²⁴ INS staff reported that this problem was corrected as soon as they became aware of it.

extent that it increases the number of Federal employees and contractors who have access to its data.

- There is no indication that authorized or unauthorized use of the Basic Pilot system by employers can result in violation of employee privacy since, other than work-authorization status, the system provides no information that the employer does not already have.
- The Basic Pilot procedures were designed to safeguard access to the Basic Pilot system. Although most Basic Pilot employers maintain password security and limit access to authorized users, evidence from on-site visits suggests that there are security breaches, such as failure to secure passwords and instructions and easy access to the computer by an unauthorized user.
- Because local data files are not encrypted, the pilot software presents opportunities for privacy violations and perhaps fraud. For example, someone wishing to protect a new employee not confirmed by the system could change that employee's confirmation code from "not confirmed" to "confirmed." A confirmation notice could then be printed and placed in the employee's file. Although such irregularities could be detected by comparing the employee's status on the SSA or INS database and the status on the printed Case Detail, these comparisons are not carried out.

The failure of some employers to implement computer security procedures is a serious concern. This concern would be much greater if the Basic Pilot were implemented on a larger scale. Given the latitude employers have in using the system, the evaluation team believes that a quality control program should be instituted to review how employers use the system and to highlight possible irregularities. Under such a program, a small group of employers could be randomly selected by the system and audited to determine whether they are complying with the provisions of the MOU. This approach would further emphasize to employers the importance of following the Basic Pilot rules. Determining the exact nature of any quality control procedures to be instituted would require a careful consideration of costs.¹²⁵

¹²⁵ According to INS officials, audits and penalties have not been implemented because they would be contrary to the spirit of a voluntary pilot program and would potentially interfere with the evaluation.

